UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/023,846	12/21/2001	Keith Alexander Harrison	30003039-2	5756

7590 03/09/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
BERGER, AUBREY H	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 03/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/023,846	HARRISON ET AL.	
	Examiner	Art Unit	
	Aubrey H. Berger	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/16/2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *42-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *42-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 12/16/05 was received and considered.

2. Claims 42-56 are pending.

Response to Arguments

3. Applicant's response (page 1, ¶3) amends the specification, abstract, and title to overcome the objections set forth in the previous Office Action and therefore those objections are withdrawn.

4. Applicant's arguments with respect to claims 1-41 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 42-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muftic, U.S. Patent Number 5,745,574, hereinafter "Muftic", in view of Sweet et all, U.S. Patent Application Publication Number 2002/0031230, hereinafter "Sweet", and further in view of "Handbook of Applied Cryptography" by Menezes, hereinafter "Menezes".

Regarding claim 42, Muftic discloses a method of communicating credentials, the method comprising: a first party/U2 (fig. 4, #430), communicating a composite credential/certificate (fig. 3), across a distributed electronic network/Internet (col. 10, lines 35-37), to a second party/U1 (fig. 4, #450), wherein the composite credential/certificate, comprises a plurality of obfuscated credentials (fig. 3, #300-370).

Muftic lacks or does not expressly disclose in which different obfuscation is used for at least two credentials in the composite credential. However Sweet discloses in which different obfuscation is used for at least two credentials in the composite credential/file (¶[0143]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Muftic with the device of Sweet to use different obfuscation for at least two credentials in the composite credential because it facilitates differentiated role-based access to large collections of digital information, as taught by Sweet, (¶[0143]). Muftic further discloses the second party/U1, de-obfuscating/decrypting (fig. 5, #530 or #510) at least one credential (col. 12, lines 51-52), and communicating to a third party/CA3 (fig. 4, #420), at least one obfuscated credential from the composite credential (col. 13, lines 13-16). Muftic fails to explicitly teach that a certificate can be communicated from a CA as well as the user. However, Menezes teaches a certificate may come from a user/trusted third party, (page 39, §1.11.3). One of ordinary skill in the art would have been motivated to modify the method of Muftic with the method of Menezes to allow a certificate to come from a user because a trusted third party may have access to the secret or private keys of users and therefore send a certificate. Therefore, it would have been obvious to one of

ordinary skill in the art at the time the invention was made to modify the method of Muftic with the method of Menezes.

Regarding claims 43-45, Muftic further discloses a method of communicating credentials according to claim 42 as modified above, wherein the second party/U1, receives a composite credential/certificate, and the second party/U1, modifies the received composite credential/U1, before communicating it to the third party/CA3 (col. 12, lines 49-51), wherein the second party/U1, receives a composite credential/certificate, and the second party/U1 communicates the received composite credential/certificate, to the third party/CA3 (fig. 4), wherein all credentials are obfuscated within the composite credential/certificate (fig. 3).

Regarding claim 46, Muftic further discloses a method of communicating credentials according to claim 45 as modified above, in which different obfuscation is used for each obfuscated credential in the composite credential (Sweet, ¶[0143]).

Regarding claim 47, Muftic further discloses a method of communicating credentials according to claim 42 as modified above, wherein the composite credential/certificate, comprises a first credential and a second credential in which the second credential is enveloped by the first credential (digest, col. 12, lines 54-56).

Regarding claim 48-50, Muftic further discloses a method of communicating credentials according to claim 42 as modified above, wherein the first party/U2, communicates to the second party/U1, an obfuscated composite credential/certificate, comprising a first credential and a second credential in which the second credential is enveloped by the first credential (digest, col. 12, lines 54-56), wherein the obfuscated composite credential/certificate, is de-obfuscated/decrypted, by the second party/U1, thereby to obtain the first credential and a party de-obfuscated/decrypted, second credential, which partly de-obfuscated/decrypted, second credential is communicated by the second party/U1, to a third party/CA3, wherein the third/CA3, party de-obfuscates/decrypts, the partly de-obfuscated second credential (col. 12, lines 56-60).

Regarding claim 51, Muftic further discloses a method of communicating credentials according to claim 50 as modified above, wherein the composite credential/certificate, is at least partly obfuscated, and wherein the second party/U1, de-obfuscates a relevant credential (fig. 5, #530 or #510).

Regarding claim 52-55, Muftic further discloses a method of communicating credentials according to claim 42 as modified above, wherein at least one credential is digitally signed, in which a plurality of credentials is digitally signed, in which all credentials in the composite credential/certificate, are digitally signed, in which the composite credential/certificate, is digitally signed (col. 11, lines 36-38).

Regarding claim 56, Muftic further discloses a method of communicating credentials according to claim 42 as modified above, in which the distributed electronic network is the Internet (col. 10, lines 35-37).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. U.S. Patent Number 5,757,920 to Misra et al. is cited for encrypting a digitally signed and sealed certificate of credentials.

b. U.S. Patent Number 5,497,422 to Tysen et al. is cited for teaching a digitally signed message protected with a chain of encrypted certificates comprising a plurality of credentials.

c. U.S. Patent Number 6,131,090 to Basso, Jr. et al. is cited for communicating a composite credential to a third party for verification.

d. U.S. Patent Application Number 2002/0138728 to Parfenov et al. is cited for encrypting credentials into separate messages.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aubrey H. Berger whose telephone number is (571)272-8155. The examiner can normally be reached on Monday - Thursday, 7:30 a.m. - 5:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AHB

AHB

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100